CLAIMS

1. A method for complicating a coincidence attack in a system for protecting content on recordable media, comprising:

providing a single media key;

Transforming the media key using a position-specific function with each of a sequence of positions to render a sequence of position-dependent media keys; and

encrypting each position-dependent media key with a respective position-dependent device key.

2. A system for complicating a coincidence attack in a system for protecting content on recordable media, comprising:

a media key block (MKB), the MKB including plural encrypted entries, each entry having a position in the MKB, each entry being established at least in part by transforming the entry using a number representing its respective position.

3. The system of Claim 2, wherein an entry is established by a media key.

4. The system of Claim 2, wherein each entry is established by the same media key as all other entries, the media key being combined with each of a sequence of positions to render a sequence of position-dependent media keys.

5. The system of Claim 4, wherein each position-dependent media key is encrypted by a respective device key.

6. The system of Claim 5, further comprising plural players, each having a device key of known position with which to decrypt the media key to play content encrypted with the media key.

7. A computer program device, comprising:

a computer program storage device including a program of instructions usable by an encryption computer, comprising:

logic means for receiving a media key;

logic means for altering the media key with each of a sequence of numbers to render a sequence of media keys; and

logic means for encrypting each key in the sequence of media keys with a respective device key associated with the respective number.

8. The computer program device of Claim 7, wherein each number represents a position in a key matrix.

9. The computer program device of Claim 8, wherein the means for altering XORs the media key with at least one of the numbers to render a key in the sequence of keys.

10. A computer program device, comprising:

a computer program storage device including a program of instructions usable by a decryption computer, comprising:

logic means for receiving a media key block (MKB) having plural positions, each position having a number related thereto;

logic means for accessing a device key, the device key being associated with a position corresponding to one of the positions of the MKB, the position associated with the device key being known to the decryption computer;

logic means for decrypting the number at a position in the MKB corresponding to the position associated with the device key to render a decrypted position-dependent media key; and

logic means for reverse transforming the position-dependent media key with a number representing the position of the position-dependent media key in the MKB, to render a media key.

11. The computer program device of Claim 10, further comprising logic means for decrypting content using the media key.